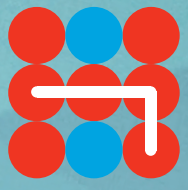
COI STRATEGY AND DEFENCE

Hybrid CoE Paper 7

JUNE 2021

Geopolitics and strategies in cyberspace: Actors, actions, structures and responses

ANTONIO MISSIROLI



Hybrid CoE

Hybrid CoE Paper 7

Geopolitics and strategies in cyberspace: Actors, actions, structures and responses

ANTONIO MISSIROLI

Hybrid CoE Papers are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

COI Strategy & Defence focuses on hybrid warfare, related strategies and resulting implications for security policy, military and defence. It aims at discovering the essence and nature of hybrid warfare as well as the logic and pattern of hybrid strategies in order to develop an analytical framework for the assessment of current and future hybrid warfare situations.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253 800 www.hybridcoe.fi

ISBN (web) 978-952-7282-82-3
ISBN (print) 978-952-7282-83-0
ISSN 2670-2053

June 2021

Hybrid CoE is an international hub for practitioners and experts, building Participating States' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats, located in Helsinki, Finland.

Contents

Introduction

Even during the COVID-19 pandemic, widespread hostile cyber-enabled activities have highlighted that no domain of public (and personal) life is now immune to geopolitical or systemic competition. In addition, it has become clear that no humanitarian consideration or collective health concern prevents the ruthless employment of sophisticated digital tools to gain an advantage and inflict damage on potential competitors and adversaries; and that the boundaries between intelligence and criminal online operations are increasingly fuzzy.

The spectrum of such hostile activities has encompassed ransomware attacks against medical facilities, intellectual property theft attempts against laboratories developing vaccines, not to mention misinformation and disinformation campaigns. They have been related to the source of the virus, the reality of the pandemic itself, the way in which individual countries were coping with it, and the potential effects of vaccination.

Without entering into the ongoing debate on whether the pandemic is a strategic game changer or just an accelerator of current trends, it is evident that hostile cyber-enabled activities have complicated the global response to COVID-19. They have also highlighted that 'cyber' (both a noun and a prefix covering a variety of digital, computer-related activities) has become ever more critical to our individual and collective security – as both an arena and a conduit – and an increasingly contested 'space' in its own right. This paper will provide an overview of why this is so, who operates in cyberspace and with what aims, and how some of the resulting security challenges are being addressed.

Conflict in cyberspace: attribution and governance

While there is no universally accepted definition,[1] cyber *securit*y consists – broadly speaking – of measures to protect cyberspace from hostile actions: nowadays, virtually every business and public institution have staff dealing with it. Insofar as such measures are within the remit of the military or impinge on military capabilities, they normally constitute cyber *defence* – although 'defence' may of course also be used more generally to convey an action rather than a specific actor. At any rate, different definitions reflect different mandates, with many variations across governments and countries: strengthening cyber 'defence' does not necessarily entail involving the military.

Cyber*space* is usually defined as all computer systems and networks in existence (including air-gapped, non-interfaced ones), while the cyber *domain* also encompasses the human and institutional actors that operate and regulate it. Cyber-related *threats* may range from armed conflict proper (more likely as part of 'hybrid' warfare, as in 2014 Ukraine) to espionage, sabotage, disruption, coercion and even subversion activities, including so-called influence operations at a domestic political level. Their consequences may lead to anything from mere annoyance to possible fatalities, up to potential threats to strategic command, control and communication systems. Not all hostile cyber activities are of equal importance, not all pose significant threats to national or collective security, and not all can be prevented. The hostile cyber operators themselves may range from states or state-sponsored groups to criminal organizations, from 'hacktivists' to terrorist franchises.

Moreover, while cyber *warfare* proper (i.e. as carried out *only* in cyberspace) still seems a remote possibility, it is difficult to imagine any future armed conflict or high-end military operation without a significant enabling or disabling cyber component (cyber *in* warfare). Furthermore, most hostile cyber activities based on the use of code do not fit neatly into the category of 'armed attack' and do not entail or elicit the use of force for self-defence, at least in a kinetic sense. It is sometimes even difficult to ascertain precisely what harm – defined as injury to or death of individuals as well as damage to or destruction of property – is the result of a cyber operation. In fact, digital technologies have dramatically lowered the entry barriers for new threat actors (the 'democratization' effect) and extended the scope and *modus operandi* of hostile activities (the 'weaponization' effect) that were already quite common, for instance, during the Cold War. Yet they have also decreased the overall level of direct *physical* violence.

Hostile cyber *activities* lying below the level of an armed attack represent comparatively low cost, low risk but high impact operations that are difficult to detect, deter and defend against. For state actors in particular, resorting to digital 'weapons' – including through proxies – is a very effective way to externalize the material and reputational costs of warfare while lowering public accountability.

The main vectors of a cyber*attack* – intended as the use of code to interfere with the functionality of a computer system for political or strategic purposes in order to damage, disrupt or destroy – are networks, supply chains and human insiders

1 The section that follows relies on a number of different sources that cannot be listed in full. For most of the definitions, however, see Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale UP, 2017), especially 44–55. For the conceptual implications for security and defence, see Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Co., 2013). For a general introduction, see Myriam Dunn Cavelty, *Cyber-Security*, in *Contemporary Security Studies*, ed. Alan Collins, 5th edition (Oxford UP, 2019), 410–426.

(malicious or just careless). Cyberattacks can be generalized (no machine connected to the internet is in principle spared), as with the 2007 attack against Estonia, or customized, as with the 2009/10 Stuxnet operation against Iran's nuclear programme, notably the Natanz power plant. They can be stand-alone operations or part of broader and well-coordinated destabilizing and disruptive activities. They may entail cyber exploitation, namely the penetration of an adversary's computer system for the purpose of exfiltrating data (a quintessential espionage activity also practised by Western agencies and governments); yet they may also lead to the disablement of the adversary, which amounts to sabotage (a potential *casus belli*). More often than not, they cross multiple jurisdictions, blurring the distinction between the domestic and the foreign sphere. Their opacity also blurs the distinction between crime and war as well as between peace, crisis and conflict: there are no tanks crossing borders, no visible insignia or soldiers, no debris or minefield ('what you *cannot* see is what you get'). Moreover, attacks can occur anytime and anywhere: the attack surface is virtually infinite.

As a result, attributing a cyberattack or even just malicious activity can be a particularly complex and challenging process. It includes a sophisticated technical component (forensics proper, often carried out also by private companies) and, particularly for state actors, an equally sophisticated all-source intelligence component to assess circumstance and hostile intent. Deception – through spoofing and false flag techniques – is quite common in the cyber domain: even knowing the true location of the originating machine is not the same as knowing the ultimate instigator of an attack, although skilled investigators can reduce the list of potential aggressors. Attribution, in other words, is a matter of degree (it can rarely be 100% conclusive) as well as political judgement, especially when made public by governments and/or specialized agencies. Disclosing forensic methods and/or intelligence sources may actually diminish or even compromise their value for future contingencies. Not doing so, however, could open the door to plausible deniability and the potential loss of international support. In other words, while inaction and silence could signal weakness, the jury is still out as to the effectiveness of naming and shaming – in and of itself – in deterring hostile activities.

Furthermore, public attribution exposes vulnerabilities, entails reputational damage and also elicits some form of retribution, preferably with tangible consequences for the perpetrator. As a consequence, the lack of visible or credible responses may inflict reputational damage on the attributor. Attribution, in other words, is a form of strategic communication: it is about messaging (bilaterally and discreetly, or jointly and publicly), and it is about perceptions. It requires credibility at source, including the capability to retaliate. Yet retaliation in kind – that is, 'intra-domain' – is complicated by the particular nature of cyberspace (a man-made ecosystem, mostly privately owned and operated) and carries the risk of unintended consequences, collateral damage, miscalculation and escalation. So-called offensive cyber 'effects' are in fact one-shot weapons ('you launch it, you lose it'), whose ultimate impact and outreach cannot always be controlled. They can also be reverse-engineered, repurposed and reused by an adversary. What is more, all of this is amplified by the lightning speed at which action unfolds in cyberspace, which compels responders to (re)act quickly on the basis of incomplete or ambiguous information and in compromised environments.

Finally, not only is global governance of cyberspace highly fragmented,[2] but digital 'weapons' are neither banned nor controlled internationally, despite ongoing efforts at UN level to set rules of responsible state behaviour (the general norms endorsed by the General Assembly in 2015 are voluntary, non-binding and not enforceable), and attempts at OSCE level to discuss confidence-building measures and early-warning protocols. Classical arms control-type arrangements and

2 Intellectual property is dealt with in the WIPO, digital commerce in the WTO, privacy protection in the UN Human Rights Council, and IP numbers in ICANN, a non-profit legal entity incorporated in California. The Budapest Convention on Cybercrime, originally drafted within the Council of Europe and entered into force in 2004, has been ratified by 65 countries. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, originally signed in 1995, now includes a provision (2015) for systems that 'command and control' intrusion software, but not all signatories have translated it into law yet.

mechanisms indeed seem inapplicable to the cyber domain: the intrinsic ubiquity and dual-use nature of information technology would make inspections pointless, verification of stockpiles virtually impossible, and compliance hardly enforceable. Cyber assets and capabilities can be promptly and easily recreated.

Needless to say, reliable and releasable information about cyber threat actors, their strategies and their methods is for the most part difficult to access, often shrouded in (legitimate) secrecy, and quite easy to contest. Nevertheless, it is possible to sketch some profiles and to identify distinctive patterns of behaviour.[3]

3 The following section is based on information that circulates widely among analysts and experts. Compelling accounts are provided i.a. by two well-known *New York Times* reporters, namely David E. Sanger, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age* (London: Scribe, 2018), and Nicole Perlroth, *This is How They Tell Me the World Ends: The Cyber Weapons Arms Race* (London: Bloomsbury, 2021).

Cyber threat actors, actions and reactions

Organized crime has been and remains the main perpetrator of hostile cyber operations, at least in quantitative terms. Cybercrime – namely crime committed mostly or entirely by digital means – has increased and intensified during the pandemic (also due to the shift to remote working), especially through hacking attacks where victims' files are locked until a ransom is paid, often in Bitcoin. Such groups seem to operate in a decentralized fashion – unlike drug cartels or mafias – and often cultivate links to states interested in their know-how or their ill-gotten gains.

Over the past months, these activities have become hugely profitable, creating a peculiar business called Ransomware as a Service (RaaS) run through the Dark Web and based on renting out malware and taking a cut in the earnings. The recent Colonial Pipeline hack, which blocked the petrol supply across the southern and southeastern US (and has been attributed to Dark Side, a gang of Russian-speaking hackers based somewhere in the territory of the former USSR), is a typical case in point. Law enforcement and counter-intelligence agencies are struggling to keep up with this constantly evolving and growing threat and are considering specific forms of deterrence, including compelling targeted companies to report attacks, delaying or blocking ransom payments altogether, or 'doxing' the perpetrators, namely making their details and coordinates publicly available.[4]

So far, terrorist groups and militias have mainly used cyberspace for recruitment, funding, as well as operational purposes in-theatre (the Levant, Libya), in Europe and elsewhere. While there is still no evidence or credible prospect of cyber-terrorism proper, there is concern about the possible use of unmanned vehicles for jihadist attacks in urban environments, and cyber-enabled sabotage operations against transport or energy infrastructure. Yet most analysts believe that such activities could be carried out only with the backing of capable state or state-sponsored actors.

None of these groups, in fact, normally qualify as an Advanced Persistent Threat (APT), that is, as an actor equipped with the full spectrum of intelligence-gathering techniques, pursuing specific objectives rather than just opportunistically seeking information for financial or other gain, and guided by both intent and capability, namely executing attacks by coordinated human actions rather than mindless and automated pieces of code. The best known APTs identified so far are Russia-based Fancy Bear (also known as APT 28), Cozy Bear (APT 29), and Sandworm; a number of China-based APTs (often nicknamed Pandas) supported by either the People's Liberation Army or the Ministry of State Security; North Korea's Lazarus Group (APT38); and Iran's APT 39.

Their strategies and techniques, however, differ significantly.[5] North Korea's APTs focus mainly on criminal-type operations designed to seize financial resources for the cash-stripped regime, as in the case of the 2016 SWIFT bank 'heist' and the 2017 WannaCry ransomware. Yet they have also carried out politically symbolic cyberattacks like the one against Sony Pictures, in 2014, to prevent the company from releasing a film on the DPRK regime – the first cyber incident to be formally sanctioned and publicly attributed by the US government. Deterring groups like Lazarus, however, remains

4 See the interview given by the former US cyber security 'tsar', Chris Krebs, to the *Financial Times* (6/7 February 2021, 3) after being fired by President Trump for certifying the regularity of the November 2020 elections. See also 'Spam, scam, scam, scam', *The Economist*, 8 May 2021, 53–54, and Misha Glenny, 'Colonial cyberattack is a warning of worse to come', *Financial Times*, 15/16 May 2021, 9.
5 For a detailed description of the main APTs and their *modus operandi*, see for instance the website of FireEye, one the most famous private cyber security companies, www.fireeye.com; as well as the 2021 Global Threat Report released by Crowdstrike, another well-known private company, www.crowdstrike.com. Unless otherwise indicated, all links were last accessed on 18 June 2021.

challenging due to North Korea's minimal reliance on public networks.

Iran's posture is highly political. On the one hand, Tehran was the first victim of a targeted cyberattack (Stuxnet), later attributed by international media to a joint US-Israeli intelligence operation. On the other hand, Iranian actors are considered to have been behind the compromising of the Saudi Aramco oil company in 2012, as well as the distributed denial of service (DDoS) attack against the Sands Casino in Las Vegas in 2014, owned by pro-Israel billionaire Sheldon Adelson. Other targets are, predictably, the US and the domestic opposition to the regime.

Russian actors – which also include the (in) famous Internet Research Agency based in St. Petersburg as well as a number of contractors – tend to act geopolitically, with a disruptive and/or strategic intent, combining opportunistic and carefully tailored campaigns. Their range of operations has gone from compromising the networks of the World Anti-Doping Agency (WADA) and the Organisation for the Prohibition of Chemical Weapons (OPCW), which failed spectacularly in October 2018, to the 2017 NotPetya supply-chain attack that inflicted huge financial damage on the world economy, as well as from 'hack-and-leak' and political interference operations against democratic processes (e.g. in the US in 2016 and France in 2017) to large-scale disinformation and misinformation campaigns through social media worldwide. Russian 'Bears' are widely credited with a high degree of technical sophistication and ingenuity, a focus on strategic targets (including energy infrastructure and military command and control systems), and a remarkable ability to create havoc and engineer new ways of doing old things,[6] albeit within the context of cyberspace as we know it.

One of the most recent and alarming cases has been the SolarWinds software exploitation that affected government and business networks around the world in late 2020. A typical supply-chain attack, the SolarWinds hack was soon attributed by experts and officials to Nobelius, a group backed by Russia's Foreign Intelligence Service that was previously linked to the theft of emails from the Democratic National Committee ahead of the 2016 US presidential election – also showing how the boundaries between economic, political and security data exploitation and theft are fading.[7] On the one hand, Moscow tolerates (and occasionally uses) hackers who operate from Russia but not against Russia – only or primarily against Western interests. On the other, there seems to be little evidence of bilateral cooperation or coordination between hostile state actors proper – only efforts at disguising the origin of attacks and shifting the blame onto others.

By contrast, Chinese state and state-sponsored 'Pandas' have long focused on cyber espionage aimed at commercial gain (including through intellectual property theft), then on asset acquisition and network control (first along the New Silk Road and then worldwide), and have only recently become more assertive also in the global battle of narratives, especially after the COVID-19 outbreak. China, however, is explicitly aiming not only at comprehensive technological predominance in the medium term, but also at (re)shaping cyberspace and the internet. The Chinese 'model', as opposed to the still dominant Californian model, is centred upon the so-called Great Firewall at home and technological control abroad and relies on huge manpower and close coordination between state authorities and private players, thus potentially threatening US cyber superiority and fostering a 'bipolar' cyberspace.

The ongoing discussions and deliberations at UN level – both within the Group of 25 Governmental Experts (GGE) appointed by the Secretary-General and in the Open-Ended Working Groups (OEWG) created by the General Assembly – already reflect this growing tension between different approaches to cyberspace, its regulation and future governance. More specifically, they reflect the polarization between 'sovereign'-minded countries (led by China and Russia) and a 'Western' group advocating an open, free and rules-based digital world with a large spectrum of states still lingering in between.

6 See Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).
7 See Hannah Murphy et al., 'Cyberspace's 'silent cold war'', *Financial Times*, 19/20 December 2020, 6; Hannah Murphy, 'Russians behind *SolarWinds* hacking target 150 global foreign policy bodies', *Financial Times*, 29/30 May, 2021, 1; Marcus Willett, 'Lessons of the *SolarWinds* Hack', *Survival*, vol. 63, no. 2 (April–May 2021): 7–26.

Geopolitics in and of cyberspace: power(s) and players

Geopolitical and systemic competition thus occurs also in (and through) cyberspace, albeit with distinctive characteristics. To start with, the prefix 'geo' should not be taken literally, as physical territory is not really relevant in this context. Moreover, the 'great powers' at play here are not limited to state actors: the Big Tech commercial companies from the US West Coast and mainland China already enjoy a level of influence (and even status) often associated with statehood. Digital services providers worldwide are also relevant players, as are those non-governmental organizations and civic associations that signed off on the 2018 Paris Call for Trust and Security in Cyberspace, for instance, and those now involved in the Geneva-based CyberPeace Institute.[8]

Furthermore, the interaction between the private and public sectors varies across the world, with the US and China – yet again – as the main poles and opposite models. Finally, the underworld of 'black hat' hackers and cyber buccaneers is also part of the big picture.[9] Rather than a balance of *power*, in other words, it would be more appropriate to look at a balance of *players*.

Among state actors, cyber power overlaps only partially with other conventional indicators of capability and influence, including size and international outreach. Most assessments place the US (through the NSA), Israel (i.a. Mossad's Unit 8200), China and Russia in the top tier, with the UK (GCHQ) close behind, and Iran and North Korea considered very dangerous. Within the political West, Japan, South Korea, Australia and Canada are also seen as quite capable players, also thanks to their intelligence cooperation with the US. Inside the European Union, alongside France and Germany, most Nordic and Baltic countries as well as the Netherlands normally get very good grades. Yet such assessments also show the ever-widening digital gap between the haves and the have-nots, which makes the Global South a potential battleground for geopolitical and technological influence between the competing camps – and not only at the UN.

In the arguably most ambitious and comprehensive effort so far to conceptualize and measure cyber capability, the National Cyber Power Index released last year by Harvard's Belfer Center takes into consideration a set of criteria at 'all-of-country' level for 30 states worldwide, including government strategies, capabilities for defence and offence, resource allocation, workforce, innovation, and the private sector. As a result, virtually all of the countries mentioned above end up in the top ten cluster, bar Iran and North Korea, which score very well, however, among those using cyber for surveillance and control purposes.[10]

The emphasis on *offensive* cyber capabilities – which cover the full range of active operations, regardless of whether they are run by civilians or the military – is quite recent and reflects growing frustration over the proliferation of hostile activities for the past few years. Despite different interpretations of the applicability of international law (including humanitarian law) to cyberspace, most experts believe that it is already entirely possible to justify retorsions for such activities and even to apply – on certain conditions – countermeasures that do not include the use of force.[11] Most importantly, such responses need not be limited to the

8 See: Paris Call, https://pariscall.international/en/; and CyberPeace Institute, https://cyberpeaceinstitute.org.
9 See Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge UP, 2018).
10 See Julia Voo et al., *National Cyber Power Index 2020*, Belfer Center for Science and International Affairs, Harvard University, September 2020. The International Telecommunications Union (ITU), which is part of the UN, also publishes a Global Cybersecurity Index (the latest in 2018) based, however, on self-assessments.
11 While the initial broad consensus reached at UN level with the 2013 and especially the 2015 GGE Reports on the general applicability of international law to the use of digital technologies has gradually waned, significant work has been carried out at academic level through the two iterations of the so-called 'Tallinn Manuals': see Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge UP, 2013); and Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge UP, 2017).

cyber domain. On the contrary, several national strategies now make reference to diplomatic, information, military, economic, financial, intelligence and legal (DIMEFIL) measures as part of a comprehensive, 'cross-domain' toolbox.

At multilateral regional level, both the European Union (EU) and NATO have equipped themselves to prevent, mitigate and respond to hostile cyber activities by building on their respective strengths and mandates. The EU has exercised its regulatory powers – starting with the Network and Information Systems (NIS) Directive[12] and the Cybersecurity Strategy,[13] both recently updated – and has set up a dedicated Cyber Diplomatic Toolbox[14] that allows sanctions to be imposed on specific targets (an option that has already been used on a couple of occasions).

For its part, NATO has adopted stricter technical criteria for its own networks and beefed up its Baseline Requirements to ensure the resilience of critical national infrastructure. The Alliance has also agreed a Guide for Strategic Response Options to Significant Malicious Cyber Activities (those lying below the level of armed conflict), created a mechanism for integrating some offensive cyber tools – the so-called Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) – into its missions and operations,[15] and launched a review of its 2014 Enhanced Cyber Defence Policy.

Last but not least, beyond EU regulation and NATO standardization, in February 2016 the computer emergency/incident response teams of the two organizations (CERT-EU and N-CIRC) signed a bilateral Technical Agreement on the exchange of information about threat actors and techniques, and cyber elements have regularly been incorporated into crisis management exercises involving the Union and the Alliance.[16] Cyber-related intelligence sharing and capacity building with partner countries have also increased significantly and take place more informally between government agencies.

12 See European Commission, 'NIS Directive', May 2021, https://digital-strategy.ec.europa.eu/en/policies/nis-directive.
13 European Commission, 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient', Press release, 16 December 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.
14 European Union, *Cyber Diplomacy in the European Union*, 2019, https://eucyberdirect.eu/wp-content/uploads/2019/12/cd_booklet-final.pdf.
15 Several Allies have already made their national 'effects' available, in principle, to Supreme Allied Commander Europe (SACEUR), while a Cyber Operations Center (CyOC) has been set up at NATO Military Headquarters in Mons. For NATO documents related to cyber, see https://natolibguides.info/cybersecurity/documents.
16 More detailed information about these EU and NATO initiatives can be accessed through their respective websites.

Conclusion

Taken together, all of these measures may not amount to *strategic* deterrence as we know it – namely the classical combination of denial and punishment – if anything, because in the nuclear domain weapons are not meant to be used, while in the cyber domain they are constantly used. Yet they may contribute to *tailored* deterrence by appropriately combining a higher degree of denial (resilience), propensity to expose and stigmatize (attribution), and readiness for punishment (not necessarily in kind); by constantly adapting defences to one's own vulnerabilities and the type of threat actors involved; and by calibrating responses accordingly. Rather than reacting to each individual hostile action or specific effect, for instance, it may prove strategically more efficacious to respond – preferably jointly and in a coordinated fashion – to repeated actions and cumulative effects by the same perpetrator.

After all, policy cooperation and convergence among like-minded countries is also necessary to support and facilitate global efforts to preserve a free, open and secure cyberspace and to deter – or at least discourage and contain – operations like those experienced during the pandemic. If digital weapons cannot be banned, at least certain targets and techniques could, and indeed should.

Author
Dr Antonio Missiroli is a Senior Policy Fellow at the University of Leiden and a Non-Resident Associate Fellow at the NATO Defence College in Rome. Previously, he was Director of the EU Institute for Security Studies in Paris (2012–17) and NATO Assistant Secretary-General for Emerging Security Challenges (2017–2020).


Hybrid CoE